# KNOW YOUR BUSINESS PARTNER POLICY

## 1 INTRODUCTION

### 1.1 Business Partners - Integrity Due Diligence

The purpose of this Policy is to describe our Company's objective and efforts to reduce risk in relation to business partners ("**Business Partners**"). The term Business Partners includes all enterprises or individuals our company enters into a business relationship with, including banks, charterers, agents, brokers, ship managers, consultants, joint venture partners, suppliers and other intermediaries.

In order to gain an overview of our Business Partners and to discover potential risks of Business Partners violating sanctions, or being involved in money laundering, corruption or other non-compliant conditions, we have collaborated with Dow Jones to use their third party management tool Dow Jones RiskCenter

The purpose of using the RiskCenter is to complete and document a background check ("Integrity Due Diligence" or "IDD") by collecting key information about our Business Partners, prior to entering into any contract. Any "red flags" identified will be assessed and risk mitigating measures will be considered. The tool also provides for ongoing screening of our counterparties, such as sanctions screening.

We select our Business Partners carefully. Our Integrity Due Diligence efforts are risk-based, meaning that we will not apply the same process to all Business Partners. The level of due diligence will be determined based on the application of a systematic approach described in this procedure. Further, this procedure describes how to make use of the RiskCenter.

### 1.2 Responsibility

The Compliance Officer is responsible for the implementation and monitoring of the Know Your Business Partner Policy.

Any employee or manager that enters into new contracts with our Business Partners is responsible for compliance with this Policy and for completing the onboarding and risk assessment in respect of the Business Partner in the RiskCenter.

When a new Business Partner has been onboarded to the RiskCenter and the risk assessment has been completed, the Compliance Officer is responsible for screening, risk mitigation and approval or declining approval of the Business Partners. For High Risk Business Partners, the Compliance Officer may request approval from the CFO or the CEO.

## 2 ONBOARDING – INTEGRITY DUE DILIGENCE

### 2.1 Situations in which onboarding is required

All of our Business Partners shall be registered in the RiskCenter prior to entering into any contract, except the Business Partners listed in section 2.2.

You should also register any third party that you are aware may represent a risk for our Company, regardless of lacking a contractual relationship, e.g. ship managers or banks used by our Business Partners.

To the extent priorities must be made, priority should always be given to Business Partners that are considered as medium or high risk, such as consultants, agents and other intermediaries or counterparties operating in high risk jurisdictions, e.g. in Venezuela, North Korea, Nigeria, Iran, Syria, Russia or China.

### 2.2 Situations in which onboarding is not required

If the transactions fall under any of the categories below, onboarding is not required. The following categories are excluded from the requirement of a background check and ongoing monitoring:

- Transactions with suppliers that sell goods (equipment, hardware, machines, etc.) on the basis of standard price lists;
- Contracts with a value of less than USD 10 000 a year, with the exception of contracts with consultants, agents or intermediaries that perform work in connection with public authorities and contracts with Business Partners operating in high risk areas (countries subject to sanctions or trade restrictions or with a low score on Transparency International Corruption Risk Index - https://www.transparency.org/en/cpi). For agents involved in business development and/or work with authorities, a background check must always be performed;
- Port agents, provided that the port agent is engaged by DA-Desk;
- Contracts with related entities, affilliates or subsidiaries, such as single-purpose ship owning entities.

## 3 ONBOARDING BUSINESS PARTNERS TO THE RISKCENTER KYBP

### 3.1 Introduction

The purpose of an IDD is to collect key information about a Business Partner and to analyse and assess “red flags” that may appear. “Red flags” may be e.g. that the Business Partner is registered in a high risk country, that the Business Partner is a state owned entity, that a director is a PEP (Politically Exposed Person), that the Business Partner is on a sanction list or adverse media.

The onboarding of new Business Partners should be made in accordance with the instructions provided in the “User Guide – RiskCenter KYBP”. The term "third party" in this document, refers to the same as "Business Partner" in this Policy. You may access the RiskCenter on this link: https://auth.cericosolutions.com

Prior to accessing the RiskCenter for the first time, you must register your user and create a password for your user account. You will receive an invitation in an email from the Compliance Officer.

### 3.2 Onboarding and Risk Assessment

When onboarding a potential Business Partner, you must accurately fill in all the details required in the RiskCenter.

Prior to entering into a contract, you should ensure that you have reliable information about all

owners and beneficial owners, directors and key management and that such entities and individuals are screened within the RiskCenter. Sufficient time to gather the required information about the Business Partner must be ensured.

When onboarding information has been entered, you may review the risk level of the Business Partner.

You must also complete the risk assessment with accurate and required information. When the risk assessment has been completed, you should notify the Compliance Officer by email.

If in doubt of any steps relating to the onboarding and risk assessment, you should always consult the Compliance Officer.

### 3.3 Screening and Due Diligence

When a Business Partner has been onboarded to the RiskCenter and the risk assessment has been completed, the Compliance Officer is responsible for screening and assessing potential red flags, including completing the Risk Mitigation within the RiskCenter. The Compliance Officer performs the screening and due diligence in cooperation with the user that has onboarded the Business Partner in question.

If the risk level is "high", either in respect of the primary entity (the Business Partner) or any of its related entities, owners, ultimate beneficial owner or directors, an Infospectrum report may be ordered as part of the due diligence by the Compliance Officer for further assessment.

The Compliance Officer may also request an external Integrity Due Diligence report from a third party vendor.

In respect of some Business Partners, the involvement of outside legal counsel may be required, e.g. for advice relating to US sanctions and in respect of high risk Business Partners or trading areas.

The amount of effort to be expended must be determined based on the red flags identified, contract value, our Company's exposure and the facts of each contractual relationship.

### 3.4 Approval

When all the required steps within the RiskCenter have been completed in respect of a Business Partner, the Compliance Officer is responsible for approving or declining approval of the Business Partners. For High Risk Business Partners, the Compliance Officer may request approval from the CFO or the CEO.

## 4 RISK MITIGATION AND MONITORING

You are responsible for completing any required risk mitigating actions, such as:

- Asking high risk Business Partners to comply with our Code of Business Ethics and Conduct;
- Using updated and adequate contract clauses related to anti-corruption, trade sanctions, cargo origin, AIS dark activity, labour standards etc. and monitor compliance with such contract clauses;
- Requiring compliance/anti-corruption training of certain Business Partners;

- Requiring audit rights of the Business Partners;
- Ensuring termination rights and the right to suspend further payments if there is a suspicion of irregularities or confirmed non-compliance with applicable laws and regulations;
- Performing a thorough review of invoices and the work performed by the Business Partner

You will receive alerts from the Compliance Officer if the risk level associated with the Business Partners you have onboarded to the RiskCenter changes. You are responsible for complyting with such changes and to initiate mitigating steps.

If in doubt, you should always consult the Compliance Officer. The Compliance Officer shall provide any assistance required in respect of the above.

## 5 DATA PRIVACY IN RELATION TO THE RISKCENTER

Although information collected in respect of an IDD normally relates to businesses, and not individuals, the IDD will generally involve the processing of personal data.

The Company must ensure that any collected personal data under this KYPB Policy are adequate, relevant and not excessive in relation to the purpose for which it is gathered. The categories of the personal data to be collected and processed in connection with IDD processes will vary depending on the case at hand. The Company may in this respect process sensitive personal data, including information on the suspicion of criminal conduct, e.g. breach of laws applicable to accounting, bribery, corruption, discrimination and health, the environment and security. Further, we may process information on whether employees or consultants have any relations to government entities or political parties. Although such data may not be considered sensitive under applicable data privacy laws, we must strive to treat them as sensitive.

The result of an IDD will be shared on a need-to-know basis. IDD documents and reports will be kept by the person responsible for conducting IDDs and the Approval Group as deemed necessary and only shared with employees that have a work-related need to access such documents.